UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/855,818	05/15/2001	Gerald R. Malan	UOM0206PUSP	9686

7590 04/26/2006

EXAMINER
GELAGAY, SHEWAYE

ART UNIT	PAPER NUMBER
2137	

David R. Syrowik
Brooks & Kushman P.C.
1000 Town Center, 22nd Floor
Southfield, MI 48075-1351

DATE MAILED: 04/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/855,818	MALAN ET AL.	
	Examiner	Art Unit	
	Shewaye Gelagay	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 February 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,7-12,15 and 16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,7-12,15 and 16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *12/8/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

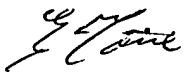
1. In view of the Appeal Brief filed on 1/17/06, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.1 1 1 (if this Office action is non-final) or a reply under 37 CFR 1.1 13 (if this Office action is finall; or,

(2) request for reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, aïdavits (37 CFR 1.130, 1. 131 or 1.132) or other evidence are permitted. See 37 CFR 1.193 (b)(2).

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below: 

2. Claims 1-4, 7-12 and 15-16 are pending.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

4. Claims 1-4 and 9-12 are rejected under 35 U.S.C. 102(a) as being anticipated by Kato et al. "A Real-Time Intrusion Detection System (IDS) for Large Scale Networks and Its Evaluations", (hereinafter Kato) pages 1817-1825.

As per claims 1 and 9:

Kato discloses a method for protecting publicly accessible network computer services from undesirable network traffic in real-time, the method comprising:

receiving network traffic including a stream of service requests destined for the publicly accessible network computer services; (page 1817, col. 2, paragraph 5; Page 1818, paragraphs 2-3, 5)

generating request statistics including connection statistics and service and service request distributions based on the stream of service requests; (page 1817, col. 2, paragraphs 2-3; page 1820, col. 2, paragraph 1)

analyzing the request statistics to identify an undesirable user of the services; (page 1817, col. 2, paragraphs 2, 3; page 1818, col. 1, paragraph 1; page 1820, col. 2, paragraph 1); and

limiting or removing access of the identified undesirable user to the services to protect the services.(page 1817, col. 2, paragraph 5; page 1821, Col. 2 paragraph 1)

As per claims 2 and 10:

Kato teaches all the subject matter as discussed above. In addition, Kato further discloses a method wherein the undesirable network traffic includes denial of service attacks. (page 1818, Col. 1, paragraph 6-col. 2, paragraph 2)

As per claims 3 and 11:

Kato teaches all the subject matter as discussed above. In addition, Kato further discloses a method wherein the network is the Internet. (Figure 1; page 1817, col. 2, paragraph 5)

As per claims 4 and 12:

Kato teaches all the subject matter as discussed above. In addition, Kato further discloses a method comprising generating one or more user profiles from the request statistics wherein the step of analyzing includes the step of comparing the one or more user profiles with a predetermined profile to determine the undesirable user. (page 1817, col. 1, paragraph 1; page 1821, col. 2, paragraph 1)

5. Claims 7-8 and 15-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kato et al. "A Real-Time Intrusion Detection System (IDS) for Large Scale Networks and Its Evaluations", (hereinafter Kato) pages 1817-1825 and further in view of Smith, R. N. et al. (hereinafter Smith) ("Operating Firewalls Outside the LAN Perimeter").

As per claims 7 and 15:

Kato teaches receiving network traffic including a stream of service requests where the network is the Internet and generating request statistics based on the stream of service requests as discussed above. Kato does not explicitly disclose of generating request statistics includes the steps of collecting and correlating Border Gateway Protocol (BGP) data from the Internet to obtain the service request distributions. (Page 497, Col. 1, Parag. 2 ; and Col. 2, Parag. 2)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Kato to include generating request statistics includes the steps of collecting and correlating Border Gateway Protocol (BGP) data from the Internet to obtain the service request distributions. This modification would have been obvious because a person having ordinary skill in the art would have been motivated in order to implement filtering function of packets and determine hope count when routing a packet. (page 497, col. 1, paragraphs 1-2; Smith)

As per claims 8 and 16:

The combination of Kato and Smith teaches all the subject matter as discussed above. In addition, Kato further discloses a method wherein the step of correlating includes the step of identifying a topologically clustered set of machines in the Internet based on the data and wherein the service request distributions are generated from the set of machines. (Figures 8 and 9; page 1820, col. 2 paragraph 2-page 1821, col. 1)

6. Claims 1 and 9 are rejected under 35 U.S.C. 102(e) as being anticipated by Belissent U.S. Patent 6,789,203.

As per claims 1 and 9:

Belissent teaches a method for protecting publicly accessible network computer services from undesirable network traffic in real-time, the method comprising:

receiving network traffic including a stream of service requests destined for the publicly accessible network computer services; (Col. 2, lines 55-56; Col. 4, lines 15-17)

generating request statistics including connection statistics and service request distributions based on the stream of service requests; (Col. 2, lines 55-59; Col. 4, lines 18-19)

analyzing the request statistics to identify an undesirable user of the services; (Col. 2, lines 59-65; Col. 4, lines 18-20); and

limiting or removing access of the identified undesirable user to the services to protect the services.(Col. 5, lines 45-51)

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See Form PTO-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shewaye Gelagay
4/19/06

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER